Privacy Vaults Online, Inc., d/b/a PRIVO
17949 Main St., #1025
Dumfries, VA 22026

PRIVO.com

5Rights Foundation

Lessons Learned from COPPA

May 16, 2019

Contact:

Claire Quinn
VP of Compliance
83 South Street
Dorking
Surrey
UK
RH4 2JU
[redacted]
www.privo.com

The United States Children's Online Privacy Protection Act of 1998, COPPA, was designed by lawmakers to introduce parents into the decision-making equation and place them in control over what information is collected online from their children. The intent of the law was to give parents the final say on which online services their children would be allowed to personally interact with and what information they could share or disclose.

Since its inception, complying with COPPA has created headaches for online content providers and others seeking to collect children's personal information for marketing and other purposes, as well as for parents who feel imposed upon to verify themselves as an adult over and over to allow their child to engage with the online property. Children and their parents need education about their rights and tools to support privacy in the digital world.

To avoid the law, children have learned to lie about their age, hindering the integrity and accuracy of data. Parents encourage their child to 'age up' in-order to avoid the online parental verification process. Online properties turn away children under the age of thirteen (U13) even though they are aware that those children exist in their databases and communiites, and that they are aging up against a false starting age.

When children magically 'age up', websites, apps and online services in general have no idea the age of or who the real user is and thus, the child leaves themselves in a vulnerable position for inappropriate or aggressive ad serving, access to adult content and perhaps, finding themselves in online communities that have no monitoring practices or protections.

COPPA has had a chilling effect on how industry giants and those learning from them choose to handle young visitors and users of their products and services. Despite the law and its subsequent tweaks, concerns still exist because of COPPA's way of handling different levels of parental consent, making it burdensome for companies and parents. As a result, many clicks-and-mortar businesses avoid dealing with kids online altogether missing out on a revenue stream and a chance to build their brands by turning their back on an important market segment: children and their parents. A sliding scale of assurance is required building on the sliding scale of consent under COPPA. This would help prevent the marginalisation of children when the bar to verify appears to high.

Call to Action

Fostering a privacy preserving digital ecosystem that encourages organizations to safely and responsibly engage with children and families is paramount not just for legal compliance, but for building a strong brand. The following actions would support this:

Accredidation/Safe Harbor Program

The European Data Protection body should finalise the criteria for certification programs which are a mechanism to demonstrate compliance and demonstrate brand integrity. US regulators, both federal and state, have recognized COPPA safe harbor programs. To date details of accreditation programs for the GDPR are still being debated. PRIVO urges that such certifications be recognized across the EU and not on a state by state basis. Approval from the data protection authorities of each individual Member State would not only prove costly, but would hinder business. Consumers deserve to rely on accredited trust marks when visiting online sites, apps and using connected devices.

Standadise Consent

A standardised consent process for holders of parental responsibility should be adopted to ensure a level playing field both for the children and parents and for industry. This would support the free flow of data across borders. Streamlining process while maintining trust is vital for success.

Age Screen vs Age Verification

Screening for age with an age gate works when the personal data collected and processed is “low” risk and pre moderated using a combination of software and human review. There are two market leaders in the children’s space in this field in play today. The sliding scale of consent under COPPA is a useful approach to the level of screening and verification required if used correctly and enforced, see Appendix 1.

Age screens are not appropriate when an Information Society Service wants to block a child, refer to the introductory paragraphs in this document. For example, Facebook and WhatsApp collect and process the personal data of children that by pass the age screen and this puts the child at risk on a number of privacy and safety levels.

Age verification is key but so is accountability. To date a neutral age screen that is compliant with COPPA can be used to screen u13s. Social platforms have actual knowledge that children under the age of 13 are highly active but have not had to take steps to verify the users.

Senator Markey’s Bill to amend COPPA includes the addition of Constructive Knowledge replacing Actual. However, if Actual Knowledge has not been enforced under COPPA in the case of for example Facebook and Google (YouTube) then PRIVO questions how constructive knowledge would resolve the issue of children ageing up.

T&Cs Used as a Get Out of Jail Free Card and Enforcement

Numerous Information Society Services (ISS) use language in the terms to state: "you must be 13 or older" and fail to guard against the risks of children "gaming" age screens. Lack of enforcement of the COPPA has allowed many ISS's to use the terms as a "get out of jail" card. The Actual Knowledge standard has not been enforced. Enforcement is not the only answer to creating a privacy and safety enhanced online environment for children, but it is an important one. Lack of enforcement has led the big tech giants to set the scene, if they don't take action the small and medium business do not follow.

Innovation

Compliance does not stifle innovation. Blocking children can mean infringing a child's rights to access and a missed opportunity. Build trust and integrity with parents and children and lifetime value and engagement grow. Allow the child to build an online identity that evolves through minor to adult supported by age appropriate privacy by design and default at each stage. Compliance is not just avoidance of fines and enforcement action but brings benefits to a business. The example of Toca Boca apps is one such case where the business has achieved great success while protecting the privacy and safety of young users.

The sliding scale is a useful approach to balancing the need to meet or exceed the standards that should be in place to protect children. It also helps to streamline and provide a path to engage the parent at various levels before asking them to take a more committed step to consenting to their child. Email+ would be much stronger if the + had to take a different form than email. Adopting COPPA's reasonable methods in light of available technology is an important component of allowing innovation and advancement for privacy protection. See Appendix 1.

Further information on identity and age verification

PRIVO has an identity and consent platform developed in associate with NIST under a White House Grant and was recently asked to provide recommendations to Vivace. Vivace is an Accelerated Capability Environment (ACE) funded by the Home Office.

The following is an extract from the documentation.

The industry standard today is that adults verify their identity and claim a relationship to a child whereby they vouch for the child's minor status, age range, date of birth, etc. Not all services need actual age of their young users.

Minors identity verification is not widely available. First and foremost, the data aggregators that service the companies doing adult identity verification, purposely do not include minor data. However, minors and their relationship to their parent lives in databases, for instance in education, insurance, after school programs, sport leagues, etc. The trick is to have a framework for being able to deliver and manage online identity verification and consumption that has already been reliably established in the offline and online world.

For example, PRIVO is currently validating educators within a school system who are willing to vouch for a student's grade level and provide an authoritative source to the corresponding parent/guardian email or phone to deliver privacy notices and manage consent for a NASA Challenge. These students and responsible adults are on-boarded and provided with a verified credential for re-use, allowing the broader platform and approved parties to rely on this process and reduce the need for additional age verification that would require the collection of more personal identifiable information.

Challenges

- Adults are not accustomed to verifying their identity for most opt-in engagement opportunities online, providing no foundation for the request to do this for their children.
- Children do not know their parent's online contact information.
- Parents in the US have not been educated to their parental rights and responsibilities online and don't even know COPPA exists.
- Many companies claim their sites and services are not intended for children and therefore utilize an age gate to block children.
- Children have learned to lie about their age online to avoid being blocked.
- Providing privacy protections that require age or identity verification that needs to utilize personal information is at odds.
- Verifying identity and managing the release, consent and revocation, service by service is burdensome for the end user.
- Verifying an individual adult as an actual parent/guardian, especially when children initiate the process.
- People do not always trust the verification process or feel comfortable with it.
- In some cases, parents are not interested in associating themselves to their child's online activities for fear of the unknown and the legal obligations.

Recommendations

- Build government support though awareness, restricted data access and enforcement.
- Drive industry discussion around interoperability based on standards.
- Public awareness, including a PR campaign to consumers educating them about their rights and responsibilities and what to expect from companies adopting best practices.
- Provide industry a safe sandbox to test and deploy solutions.
- Allow innovators to bring their methods to the platform (plug and play).
- Provide consumer choice of methodologies they feel comfortable with.
- Leverage existing already verified identities.
- Allow vouching system for parent child relationship.
- On-boarding offline relationships.
- Demonstrate parental consent at internet scale.
- Todays' minors will become adults who have a verified identity associated to an interoperable credential that can be consumed by relying parties.

Appendix 1

COPPA Permissions Chart		
Permissions Mechanism	**Explanation**	**Examples in Use**
No Consent	If an operator does NOT collect personal identifiable information (PII), there is no legal requirement to notify parents or obtain consent.	Pre-moderated*: - Chat - Message boards - Comment/Review - Public communications - Compliant invite a friend - Saved avatar - Creations based only on pre-determined assets - Leaderboards - Local push notifications sent by the app only, not remotely from a server **Pre-moderated should result in all PII being removed*
Notice & Opt Out: Passive Consent	COPPA allows for an operator to request a parent email to simply notify them that the child has joined and that no PII is or will be collected and no consent is required. Where the purpose of collecting a parent's online contact information is to provide voluntary notice to, and subsequently update the parent about, the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(2).	- Password reset - Account administration - Leaderboard
Email Plus +	If an operator wants to collect a child's personal information for internal purposes only, the operator may use "email plus" to obtain parental consent before collecting. **Notice to Parents:** The direct notice to the parent must request that the parent provide affirmative consent for the collection and use of the child's personal information. Affirmative consent could be clicking a link in the email as an opt in or validation. **The Plus:** Email Plus also requires that an operator take an additional step after receiving the parent's email consent to confirm that it was, in fact, the parent who provided consent.	Customized/Personalized: - Newsletters - Website experiences - Content - Alerts - Loyalty clubs - Wish lists to share - Purchasing power Personalized marketing across your own sites and apps/services only - Behavioral advertising - Product recommendations - Promotions - Profile-based news - Targeted ads

	The Plus Options: An operator can satisfy the "plus" requirement in one of two ways: 1. Requesting in the initial email seeking consent that the parent include a phone or fax number or mailing address in the reply email, so that the operator can follow up to confirm consent via telephone, fax, or postal mail; or 2. After a reasonable time delay, sending another email to the parent to confirm consent. In this confirmatory email, the operator should include all the original information contained in the direct notice, inform the parent that he or she can revoke the consent and how to revoke the consent.	Remote push notifications sent from a server Collection/Upload by and from a child: - Pictures/images - Video and audio - Private submission of UGC for a contest or to share with parent ***This media cannot be disclosed or published (i.e. cannot share with a grandparent, parent's Facebook page or teacher)*
Full Verifiable Parental Consent	If an operator is going to disclose children's personal information to third parties, or make it publicly available through operation of an online service, then the operator must use one of the more reliable methods to obtain verifiable parental consent enumerated in the Rule: **Fax, Mail or Digital Scan:** Provide a form for the parent to print, fill out, sign, and mail or fax back to the operator (the "print-and-send" method) **Credit/debit card transaction, or other online payment system:** Require the parent to use a credit card in connection with a transaction (which could consist of a membership or subscription fee, a purchase, or a charge to cover the cost of processing the credit card). **Phone / Video Conference:** Maintain a toll-free telephone number staffed by trained personnel for parents to call in their consent. **Government-issued identification:** Verifying a parent's identity by checking a form of government-issued identification against databases of such information if you promptly delete the parent's identification after completing the verification. **Verified PRIVO iD**	Unfiltered services that allow children to disclose personal information such as: - User generated content (UGC) – video, audio, images, etc. for contests, galleries and public spaces - Community features - Blog hosting services - Personal home pages - Chat rooms - Message boards - Pen pal services - Email accounts - Email-a-friend services - Sweepstakes/contest entry Personalized marketing and behavioral advertising outside of your domain
Safe Harbor Approval of new methods	Safe harbor approval of parental consent methods. A safe harbor program approved by the Commission under § 312.11 may approve its member operators' use of a parental consent method not currently enumerated in paragraph (b)(2) of this section where the safe harbor program determines that such parental consent method meets the requirements of paragraph (b)(1) of this section.	Customized registration solutions depending on needs of online service.

Exceptions to Prior Verifiable Parental Consent

1. **Need for Parental Consent**	Where the sole purpose of collecting the name or online contact information of the parent or child is to provide notice and obtain parental consent under § 312.4(c)(1). If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records.	Child's request for parent consent
2. **One Time Contact Exception**	Where the sole purpose of collecting online contact information from a child is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request.	- Homework help - Email-a-friend - Ask the expert
3. **Support for Internal Operations**	Where an operator collects a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the Web site or online service. In such case, there also shall be no obligation to provide notice under § 312.4; or Where an operator covered under paragraph (2) of the definition of Web site or online service directed to children in § 312.2 collects a persistent identifier and no other personal information from a user who affirmatively interacts with the operator and whose previous registration with that operator indicates that such user is not a child. In such case, there also shall be no obligation to provide notice under § 312.4.	- Internal analytics - Third party authentication used after age gate
4. **Safety of the Child**	Where the purpose of collecting a child's and a parent's name and online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with notice as described in § 312.4(c)(4).	- Suicide threats - Bullying threats - Aggressive behavior